Department of Defense Strategy for Operating in Cyberspace

July 2011

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Department Of Defense Strategy For Operating In Cyberspace	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department Of Defense,1400 Defense Pentagon,Washington,DC,20301**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**19**	

DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE

JULY 2011

CONTENTS

INTRODUCTION 1

STRATEGIC CONTEXT 2

FIVE STRATEGIC INITIATIVES

Strategic Initiative 1: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential 5

Strategic Initiative 2: Employ new defense operating concepts to protect DoD networks and systems 6

Strategic Initiative 3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy 8

Strategic Initiative 4: Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity 9

Strategic Initiative 5: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation 10

CONCLUSION 13

INTRODUCTION

"Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."

- 2010 National Security Strategy

Cyberspace is a defining feature of modern life. Individuals and communities worldwide connect, socialize, and organize themselves in and through cyberspace. From 2000 to 2010, global Internet usage increased from 360 million to over 2 billion people. As Internet usage continues to expand, cyberspace will become increasingly woven into the fabric of everyday life across the globe.

U.S. and international businesses trade goods and services in cyberspace, moving assets across the globe in seconds. In addition to facilitating trade in other sectors, cyberspace is itself a key sector of the global economy. Cyberspace has become an incubator for new forms of entrepreneurship, advances in technology, the spread of free speech, and new social networks that drive our economy and reflect our principles. The security and effective operation of U.S. critical infrastructure – including energy, banking and finance, transportation, communication, and the Defense Industrial Base – rely on cyberspace, industrial control systems, and information technology that may be vulnerable to disruption or exploitation.

Along with the rest of the U.S. government, the Department of Defense (DoD) depends on cyberspace to function. It is difficult to overstate this reliance; DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe. DoD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations.

The Department and the nation have vulnerabilities in cyberspace. Our reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity – the security of the technologies that we use each day. Moreover, the continuing growth of networked systems, devices, and platforms means that cyberspace is embedded into an increasing number of capabilities upon which DoD relies to complete its mission. Today, many foreign nations are working to exploit DoD unclassified and classified networks, and some foreign intelligence organizations have already acquired the capacity to disrupt elements of DoD's information infrastructure. Moreover, non-state actors increasingly threaten to penetrate and disrupt DoD networks and systems. We recognize that there may be malicious activities on DoD networks and systems that we have not yet detected.

DoD, working with its interagency and international partners, seeks to mitigate the risks posed to U.S. and allied cyberspace capabilities, while protecting and respecting the principles of privacy and civil liberties, free expression, and innovation that have made cyberspace an integral part of U.S. prosperity and security. How the Department leverages the opportunities of cyberspace, while managing inherent uncertainties and reducing vulnerabilities, will significantly impact U.S. defensive readiness and national security for years to come.

"There is no exaggerating our dependence on DoD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field."

- 2010 Quadrennial Defense Review

DoD's Strengths and Opportunities in Cyberspace

As does the nation as a whole, DoD relies on a secure and reliable cyberspace that protects fundamental freedoms, privacy, and the free flow of information. In support of both U.S. core commitments and national security, DoD has significant strengths and opportunities in cyberspace. The U.S. military's ability to use cyberspace for rapid communication and information sharing in support of operations is a critical enabler of DoD missions. More broadly, DoD's depth of knowledge in the global information and communications technology sector, including its cybersecurity expertise, provides the Department with strategic advantages in cyberspace.

The quality of the United States' human capital and knowledge base in both the public and private sectors provides DoD with a strong foundation on which to build current and future cyber capabilities. DoD has played a crucial role in building and leveraging the technological prowess of the U.S. private sector through investments in people, research, and technology. DoD will continue to embrace this spirit of entrepreneurship and work in partnership with these communities and institutions to succeed in its future cyberspace activities.

Given the dynamism of cyberspace, nations must work together to defend their common interests and promote security. DoD's relationship with U.S. allies and international partners provides a strong foundation upon which to further U.S. international cyberspace cooperation. Continued international engagement, collective self-defense, and the establishment of international cyberspace norms will also serve to strengthen cyberspace for the benefit of all.

Cyber Threats

"The very technologies that empower us to lead and create also empower those who would disrupt and destroy."

- 2010 National Security Strategy

The Internet was designed to be collaborative, rapidly expandable, and easily adaptable to technological innovation. Information flow took precedence over content integrity; identity authentication was less important than connectivity. The Internet's original designers could not have imagined the extent of its vital and growing role for DoD and its operations. The global scope of DoD networks and systems presents adversaries with broad opportunities for exploitation and attack.

Low barriers to entry for malicious cyber activity, including the widespread availability of hacking tools, mean that an individual or small group of determined cyber actors can potentially cause significant damage to both DoD and U.S. national and economic security. Small-scale technologies can have an impact disproportionate to their size; potential adversaries do not have to build expensive weapons systems to pose a significant threat to U.S. national security.

In developing its strategy for operating in cyberspace, DoD is focused on a number of central aspects of the cyber threat; these include external threat actors, insider threats, supply chain vulnerabilities, and threats to DoD's operational ability. DoD must address vulnerabilities and the concerted efforts of both state and non-state actors to gain unauthorized access to its networks and systems.

Foreign cyberspace operations against U.S. public and private sector systems are increasing in number and sophistication. DoD networks are probed millions of times every day, and successful penetrations have led to the loss of thousands of files from U.S. networks and those of U.S. allies and industry partners. Moreover, this threat continues to evolve as evidence grows of adversaries focusing on the development of increasingly sophisticated and potentially dangerous capabilities.

The potential for small groups to have an asymmetric impact in cyberspace creates very real incentives for malicious activity. Beyond formal governmental activities, cyber criminals can control botnets with millions of infected hosts. The tools and techniques developed by cyber criminals are increasing in sophistication at an incredible rate, and many of these capabilities can be purchased cheaply on the Internet. Whether the goal is monetary, access to intellectual property, or the disruption of critical DoD systems, the rapidly evolving threat landscape presents a complex and vital challenge for national and economic security.

Some cyber threats also may come from insiders. Malicious insiders may exploit their access at the behest of foreign governments, terrorist groups, criminal elements, unscrupulous associates, or on their own initiative. Whether malicious insiders are committing espionage, making a political statement, or expressing personal disgruntlement, the consequences for DoD, and national security, can be devastating.

Software and hardware are at risk of malicious tampering even before they are integrated into an operational system. The majority of information technology products used in the United States are manufactured and assembled overseas. The reliance of DoD on foreign manufacturing and development creates challenges in managing risk at points of design, manufacture, service, distribution, and disposal.

Potential U.S. adversaries may seek to exploit, disrupt, deny, and degrade the networks and systems that DoD depends on for its operations. DoD is particularly concerned with three areas of potential adversarial activity: theft or exploitation of data; disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems.

Cyber threats to U.S. national security go well beyond military targets and affect all aspects of society. Hackers and foreign governments are increasingly able to launch sophisticated intrusions into the networks and systems that control critical civilian infrastructure. Given the integrated nature of cyberspace, computer-induced failures of power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption. DoD operations—both at home and abroad—are dependent on this critical infrastructure.

While the threat to intellectual property is often less visible than the threat to critical infrastructure, it may be the most pervasive cyber threat today. Every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies. As military strength ultimately depends on economic vitality, sustained intellectual property losses erode both U.S. military effectiveness and national competitiveness in the global economy.

Strategic Initiative 1: DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.

"Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space."

- 2010 Quadrennial Defense Review

Though the networks and systems that make up cyberspace are man-made, often privately owned, and primarily civilian in use, treating cyberspace as a domain is a critical organizing concept for DoD's national security missions. This allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests. Furthermore, these efforts must include the performance of essential missions in a degraded cyber environment.

As directed by the *National Security Strategy*, DoD must ensure that it has the necessary capabilities to operate effectively in all domains- air, land, maritime, space, and cyberspace. At all levels, DoD will organize, train, and equip for the complex challenges and vast opportunities of cyberspace. To this end, the Secretary of Defense has assigned cyberspace mission responsibilities to United States Strategic Command (USSTRATCOM), the other Combatant Commands, and the Military Departments. Given its need to ensure the ability to operate effectively in cyberspace and efficiently organize its resources, DoD established U.S. Cyber Command (USCYBERCOM) as a sub-unified command of USSTRATCOM. The establishment of USCYBERCOM reflects DoD's need to:

- Manage cyberspace risk through efforts such as increased training, information assurance, greater situational awareness, and creating secure and resilient network environments;

- Assure integrity and availability by engaging in smart partnerships, building collective self defenses, and maintaining a common operating picture; and

- Ensure the development of integrated capabilities by working closely with Combatant Commands, Services, Agencies, and the acquisition community to rapidly deliver and deploy innovative capabilities where they are needed the most.

USSTRATCOM has delegated to USCYBERCOM the responsibility for synchronizing and coordinating Service components within each branch of the military, including U.S. Army Cyber Command, U.S. Fleet Cyber Command/U.S. 10th Fleet, the 24th Air Force, U.S. Marine Corps Forces Cyber Command, and U.S. Coast Guard Cyber Command. A key organizational concept behind the stand-up of USCYBERCOM is its co-location with the National Security Agency (NSA). Additionally, the Director of the National Security Agency is dual-hatted as the Commander of USCYBERCOM. Co-location and dual-hatting of these separate and distinct

Former Defense Secretary Robert M. Gates addresses an audience during the activation ceremony of U.S. Cyber Command at Fort Meade, Maryland, May 21, 2010. DoD photo by Cherie Cullen.

organizations allow DoD, and the U.S. government, to maximize talent and capabilities, leverage respective authorities, and operate more effectively to achieve DoD's mission.

Because degraded cyberspace operations for extended periods may be a reality and disruption may occur in the midst of a mission, DoD will fully integrate a complete spectrum of cyberspace scenarios into exercises and training to prepare U.S. Armed Forces for a wide variety of contingencies. A cornerstone of this activity will be the inclusion of cyber red teams throughout war games and exercises. Operating with a presumption of breach will require DoD to be agile and resilient, focusing its efforts on mission assurance and the preservation of critical operating capability.

These efforts will be supported by the development of increasingly resilient networks and systems. In the case of a contingency involving network failure or significant compromise, DoD must be able to remain operationally effective by isolating and neutralizing the impact, using redundant capacity, or shifting its operations from one system to another. Multiple networks can add diversity, resiliency, and mission assurance to cyberspace operations. DoD is investing in research to identify options for shifting its operations to secure networks at scale and across the full spectrum of operations.

Strategic Initiative 2: DoD will employ new defense operating concepts to protect DoD networks and systems.

> *"Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient."*
>
> - 2010 National Security Strategy

The implementation of constantly evolving defense operating concepts is required to achieve DoD's cyberspace mission today and in the future. As a first step, DoD is enhancing its cyber hygiene best practices to improve its cybersecurity. Second, to deter and mitigate insider threats, DoD will strengthen its workforce communications, workforce accountability, internal monitoring, and information management capabilities. Third, DoD will employ an active cyber defense capability to prevent intrusions onto DoD networks and systems. Fourth, DoD is developing new defense operating concepts and computing architectures. All of these components combine to form an adaptive and dynamic defense of DoD networks and systems.

Most vulnerabilities of and malicious acts against DoD systems can be addressed through good cyber hygiene. Cyber hygiene must be practiced by everyone at all times; it is just as important for individuals to be focused on protecting themselves as it is to keep security software and operating systems up to date. DoD will integrate the private sector's continuous renewal method to harden its own computing devices and sustain its cyber hygiene best practices. Further, good cyber hygiene extends to the maintenance of information security, the promotion of good cybersecurity practices for users and administrators alike, secure network design and implementation, and the employment of smart and effective network and configuration management. This holistic effort will provide protection, monitoring, maintenance, design, and care for DoD networks and systems to assure their security and integrity.

U.S. Sailors assigned to Navy Cyber Defense Operations Command (NCDOC) man their stations at Joint Expeditionary Base Little Creek-Fort Story, Va. NCDOC Sailors monitor, analyze, detect, and respond to unauthorized activity within U.S. Navy information systems and computer networks. U.S. Navy photo by Mass Communication Specialist Joshua J. Wahl.

People are the Department's first line of defense in sustaining good cyber hygiene and reducing insider threats. To mitigate the insider threat and prevent dangerous disclosures of sensitive and classified information from occurring, DoD will strengthen and go beyond the current information assurance paradigm, including the exploration of new operating concepts to reduce vulnerabilities. DoD's efforts will focus on communication, personnel training, and new technologies and processes. DoD seeks to foster a stronger culture of information assurance within its workforce to assure individual responsibility and deter malicious insiders by shaping behaviors and attitudes through the imposition of higher costs for malicious activity. This cultural shift will be enabled by new policies, new methods of personnel training, and innovative workforce communications.

As malicious cyber activity continues to grow, DoD has employed active cyber defense to prevent intrusions and defeat adversary activities on DoD networks and systems. Active cyber defense is DoD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. As intrusions may not always be stopped at the network boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks.

To foster resiliency and smart diversity in its networks and systems, DoD will explore new and innovative approaches and paradigms for both existing and emerging challenges. These efforts will include development and integration in the areas of mobile media and secure cloud computing. DoD will continue to be adaptive in its cyberspace efforts, embracing both evolutionary and rapid change.

Strategic Initiative 3: DoD will partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.

"Neither government nor the private sector nor individual citizens can meet this challenge alone– we will expand the ways we work together."

- 2010 National Security Strategy

The challenges of cyberspace cross sectors, industries, and U.S. government departments and agencies; they extend across national boundaries and through multiple components of the global economy. Many of DoD's critical functions and operations rely on commercial assets, including Internet Service Providers (ISPs) and global supply chains, over which DoD has no direct authority to mitigate risk effectively. Therefore, DoD will work with the Department of Homeland Security (DHS), other interagency partners, and the private sector to share ideas, develop new capabilities, and support collective efforts to meet the crosscutting challenges of cyberspace.

In order to enable a whole-of-government approach, DoD will continue to work closely with its interagency partners on new and innovative ways to increase national cybersecurity. An example of one critical initiative is the 2010 memorandum of agreement signed by the Secretary of Defense and Secretary of Homeland Security to align and enhance cybersecurity collaboration. An enhanced partnership between DHS and DoD will improve national cybersecurity in three important ways. First, the formalized structure reaffirms the limits that current law and policy set on DoD and DHS collaboration. Second, joint participation in program planning will increase each department's mission effectiveness; specifically, it will improve a shared understanding of cybersecurity needs and ensure the protection of privacy and civil liberties. Third, the arrangement will conserve limited budgetary resources. This agreement will help DHS to best protect the Executive Branch .gov domain, work in partnership with state, local, and tribal governments, partner with the private sector, and coordinate the defense of U.S. critical infrastructure.

DoD is also partnering with the Defense Industrial Base (DIB) to increase the protection of sensitive information. The DIB comprises the public and private organizations and corporations that support DoD through the provision of defense technologies, weapons systems, policy and strategy development, and personnel. To increase protection of DIB networks, DoD launched the Defense Industrial Base Cyber Security and Information Assurance (CS/IA) program in 2007. Building upon this program, DoD is also establishing a pilot public-private sector partnership intended to demonstrate the feasibility and benefits of voluntarily opting into increased sharing of information about malicious or unauthorized cyber activity and protective cybersecurity measures.

Given the rapid pace of change that characterizes cyberspace, DoD will continue to work with interagency partners and the private sector to examine new collaborative approaches to cybersecurity. These efforts will include DoD's support of DHS in leading interagency efforts to identify and mitigate cyber vulnerabilities in the nation's critical infrastructure. Success will require additional pilot programs, business models, and policy frameworks to foster public-

private synergy. Public-private partnerships will necessarily require a balance between regulation and volunteerism, and they will be built on innovation, openness, and trust. In some cases, incentives or other measures will be necessary to promote private sector participation. DoD's efforts must also extend beyond large corporations to small and medium-sized businesses to ensure participation and leverage innovation. A collaborative national effort will develop common and workable solutions to policy problems that both increase cybersecurity and further the public good.

DoD will continue to support the development of whole-of-government approaches for managing risks associated with the globalization of the information and communications technology sector. Many U.S. technology firms outsource software and hardware factors of production, and in some cases their knowledge base, to firms overseas. Additionally, increases in the number of counterfeit products and components demand procedures to both reduce risk and increase quality. Dependence on technology from untrusted sources diminishes the predictability and assurance that DoD requires, and DoD will work with DHS and its interagency partners to better identify and address these risks. The global technology supply chain affects mission critical aspects of the DoD enterprise, along with core U.S. government and private sector functions, and its risks must be mitigated through strategic public-private sector cooperation.

Strategic Initiative 4: DoD will build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity.

"Through its foreign defense relationships, the United States not only helps avert crises but also improves its effectiveness in responding to them."

- 2010 Quadrennial Defense Review

In support of the U.S. *International Strategy for Cyberspace* and in collaboration with its interagency partners, DoD will seek increasingly robust international relationships to reflect our core commitments and common interests in cyberspace. The development of international shared situational awareness and warning capabilities will enable collective self-defense and collective deterrence. By sharing timely indicators about cyber events, threat signatures of malicious code, and information about emerging actors and threats, allies and international partners can increase collective cyber defense. Cyberspace is a network of networks that includes thousands of ISPs across the globe; no single state or organization can maintain effective cyber defenses on its own.

Deputy Secretary of Defense William J. Lynn III, left, speaks about cybersecurity at a meeting of NATO's North Atlantic Council in Brussels, Belgium, Sept. 14, 2010. DoD photo by Cherie Cullen.

DoD's international engagement will support the U.S. *International Strategy for Cyberspace* and the President's commitment to fundamental freedoms, privacy, and the free

flow of information. DoD will assist U.S. efforts to advance the development and promotion of international cyberspace norms and principles that promote openness, interoperability, security, and reliability. The Department will work with interagency and international partners to encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuade and deter malicious actors, and reserve the right to defend these vital national assets as necessary and appropriate. These efforts will sustain a cyberspace that provides opportunities to innovate and yield benefits for all.

As international cyberspace cooperation continues to develop, DoD will advance its close cyberspace cooperation with its allies to defend U.S. and allied interests in cyberspace. DoD will work closely with its allies and international partners to develop shared warning capabilities, engage in capacity building, and conduct joint training activities. Engagement will create opportunities to initiate dialogues for sharing best practices in areas such as forensics, capability development, exercise participation, and public-private partnerships. Further, the development of burden sharing arrangements can play to each nation's core strengths and capabilities; this will bolster areas where partners are less proficient, increase capacity, and strengthen collective cybersecurity.

DoD will expand its formal and informal cyber cooperation to a wider pool of allied and partner militaries to develop collective self-defense and increase collective deterrence. DoD will create new opportunities for like-minded states to work cooperatively based on shared principles; expanded and strengthened relationships with allies and international partners can maximize scarce cyber capabilities, mitigate risk, and create coalitions to deter malicious activities in cyberspace. These coalitions will serve to augment DoD's formal alliances and partnerships and increase broader cybersecurity.

Strategic Initiative 5: DoD will leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

"We will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet these challenges."

- 2010 National Security Strategy

The defense of U.S. national security interests in cyberspace depends on the talent and ingenuity of the American people. DoD will catalyze U.S. scientific, academic, and economic resources to build a pool of talented civilian and military personnel to operate in cyberspace and achieve DoD objectives. Technological innovation is at the forefront of national security, and DoD will foster rapid innovation and enhance its acquisition processes to ensure effective cyberspace operations. DoD will invest in its people, technology, and research and development to create and sustain the cyberspace capabilities that are vital to national security.

The development and retention of an exceptional cyber workforce is central to DoD's strategic success in cyberspace and each of the strategic initiatives outlined in this strategy. DoD will assess its cyber workforce, requirements, and capabilities on a regular basis. The development of the cyber workforce is of paramount importance to DoD.

The demand for new cyber personnel is high, commensurate with the severity of cyber threats. DoD must make itself competitive if it is to attract technically skilled personnel to join government service for the long-term. To achieve its objectives, DoD will focus on the establishment of dynamic programs to attract talent early, and the Department will leverage the 2010 Presidential Initiative to improve federal recruitment and hiring processes. DoD will also work with the Executive Office of the President to explore strategies designed to streamline hiring practices for its cyber workforce and exchange programs to allow for "no penalty" cross-flow of cyber professionals between the public and private sectors to retain and grow innovative cyber talent.

High School competitors represent their school against nearly 500 teams during the third round of a cyber competition in December 2010. Air Force photo by Tech Sgt. Scott McNabb.

Beyond these recruiting, education, and training initiatives, adoption and scaling of cross-generational mentoring programs will allow DoD to grow a gifted cyber talent base for future defense and national security missions. Paradigm-shifting approaches such as the development of Reserve and National Guard cyber capabilities can build greater capacity, expertise, and flexibility across DoD, federal, state, and private sector activities. Opportunities for exchanges and continuing education programs will be explored by DoD, infusing an entrepreneurial approach in cyber workforce development. Continued education and training will be hallmarks of the cyber workforce, preserving, and developing DoD's intellectual capital.

To replicate the dynamism of the private sector and harness the power of emerging computing concepts, DoD's acquisition processes for information technology will adopt five principles. First, speed is a critical priority. DoD's acquisition processes and regulations must match the technology development life cycle. With information technology, this means cycles of 12 to 36 months, not seven or eight years. Second, DoD will employ incremental development and testing rather than a single deployment of large, complex systems. Third, DoD will be willing to sacrifice or defer some customization to achieve speedy incremental improvements. Fourth, DoD's information technology needs—from modernizing nuclear command and control systems to updating word-processing software—will adopt differing levels of oversight based on the Department's prioritization of critical systems. Fifth, improved security measures will be taken with all of the systems that DoD buys, including software and hardware. No backdoor can be left open to infiltration; no test module can be left active. These principles will be a part of, and reinforced by, DoD's trusted defense systems and supply chain risk mitigation strategies. For its hardware, software, architecture, systems, and processes, DoD will take a security in depth approach to design, acquisition, and implementation of trustworthy systems.

DoD will also promote opportunities for small and medium-sized businesses, and the Department will work with entrepreneurs in Silicon Valley and other U.S. technology innovation hubs to move concepts rapidly from innovative idea, to pilot program, to scaled adoption across the DoD enterprise. DoD's cyberspace acquisition programs will reflect the adaptive nature of cyberspace; it will emphasize agility, embrace new operating concepts, and foster collaboration across the scientific community and the U.S. government as a whole.

DoD will explore game changing approaches, including new architectures, to strengthen DoD's defense capabilities and make DoD systems more resistant to malicious activity. DoD will pursue revolutionary technologies that rethink the technological foundations of cyberspace. To do so, DoD will partner with leading scientific institutions to develop new, safe, and secure cyberspace capabilities that are significantly more resistant to malicious activity.

The development of the National Cyber Range will enable the success of these and other efforts, allowing DoD, other U.S. government entities, and potentially non-U.S. government partners to test and evaluate new cyberspace concepts, policies, and technologies. Although the U.S. military routinely exercises units on target ranges and in a variety of simulations, DoD has had limited capability to simulate cyberspace operations. The National Cyber Range, which allows the rapid creation of numerous models of networks, is intended to enable the military and others to address this need by simulating and testing new technologies and capabilities.

To encourage private sector participation in the development of robust cyberspace capabilities, DoD will empower organizations to serve as clearing houses for innovative concepts and technologies, rewarding firms that develop impactful and innovative technologies. Beyond its engagement with established centers of technological excellence, DoD will leverage the innovation and agility of small businesses and entrepreneurs through initiatives such as Small Business Innovation Research (SBIR), creative joint ventures, and targeted investments and grants in emerging and untested concepts.

The nation's people, technology, and dynamism provide DoD with a strong foundation on which to build its military and civilian workforce and advance its technological capabilities. DoD will continue to develop robust cyberspace capabilities, and the Department will support interagency efforts to actively engage public and private institutions to encourage cybersecurity innovation. DoD will invest in future personnel and capabilities to achieve its cyberspace objectives and support U.S. national security.

CONCLUSION

"A failure by the Department to secure its systems in cyberspace would pose a fundamental risk to our ability to accomplish defense missions today and in the future."

- 2010 Quadrennial Defense Review

National security is being redefined by cyberspace. In addition to opportunities, DoD faces significant cyberspace challenges. The Department's military, intelligence, and business operations all depend upon cyberspace for mission success. The *Department of Defense Strategy for Operating in Cyberspace* assesses these challenges and opportunities and sets a strategic approach for DoD's cyber mission.

The Department's five strategic initiatives offer a roadmap for DoD to operate effectively in cyberspace, defend national interests, and achieve national security objectives. Each initiative is distinct, yet necessarily connected with the other four. Across the strategy, activities undertaken in one initiative will contribute to DoD's strategic thinking and lead to new approaches in the others.

By pursuing the activities in this strategy, DoD will capitalize on the opportunities afforded to the Department by cyberspace; defend DoD networks and systems against intrusions and malicious activity; support efforts to strengthen cybersecurity for interagency, international, and critical industry partners; and develop robust cyberspace capabilities and partnerships. This strategy will guide the Department's defense of U.S. interests in cyberspace so that the United States and its allies and partners may continue to benefit from the innovations of the information age.